

Management rizika a jeho fáze

Příspěvek předkládá a diskutuje postup integrovaného managementu rizika obecně využitelného při posuzování rizikovosti jakýchkoliv vojenských aktivit. Management rizika představuje současně významný proaktivní nástroj pro efektivní zajištění bezpečnosti prostředí. Úroveň bezpečnosti prostředí naopak determinuje požadavky na transformaci ozbrojených sil, neboť v tomto procesu sehrává jednu z klíčových rolí. Ve stručnosti jsou popsány jednotlivé fáze integrovaného managementu rizika, který by měl být v moderních armádách aplikován nejen na úrovni vojenských útvarů a zařízení, nýbrž i při posuzování bezpečnosti v rámci akvizic misí a regionů. Při akceptaci principu subsidiarity je takto pojatá implementace managementu rizika bází zajištění globální bezpečnosti.

1. Úvod

Priority vývoje a výstavby ozbrojených sil ČR jsou determinovány řadou faktorů, souhrnně definovaných ve vojenské strategii ČR, jež rozpracovává základní principy obranné politiky obsažené v dokumentech Bezpečnostní strategie ČR, Strategická koncepce NATO a Bezpečnostní strategie EU [1]. Vycházejí především z vyhodnocení aktuálního stavu bezpečnosti prostředí a reflektují její předpokládaný vývoj. Vyhodnocení bezpečnosti prostředí vyžaduje identifikaci kritických rizik, jejich případnou kvantifikaci a následné stanovení priorit. Kvalitní posouzení rizik je bází návrhu implementace efektivních bezpečnostních opatření, přičemž nedílnou součástí tohoto procesu je zpětně formulace požadavků na roli a úkoly, tudíž i adaptaci vývoje a výstavby ozbrojených sil.

Jedním ze základních principů zajištění adekvátní globální bezpečnosti je princip subsidiarity, který předpokládá přenesení pověření a zodpovědnosti za bezpečnost na nižší úrovně. V armádní praxi to znamená přenesení zodpovědnosti na členské státy NATO a následně až na úroveň jednotlivých vojenských útvarů a zařízení.

Zajištění požadované bezpečnosti států a uvnitř států jednotlivých regionů s akcentem na ochranu konkrétních sektorů a elementů kritické infrastruktury, kde rezort obrany sehrává relevantní roli, je v současnosti jedním z významných úkolů sledovaným jak ze strany EU, tak ve spojitosti s armádou ze strany velení NATO. V praxi se zajištění bezpečnosti dosahuje implementací environmentálních manažerských systémů (EMS) na úrovni základních subjektů jednotlivých sektorů, v armádě pak na úrovni posádek a vojenských zařízení. Důležitým proaktivním nástrojem EMS, který umožňuje kvalitní naplnění zmíněného cíle za současně efektivní alokace materiálových, finančních i personálních zdrojů, je aplikace managementu rizika, jež je však ve vojenské praxi dosud implementován jen omezeně.

2. Postup při aplikaci managementu rizika

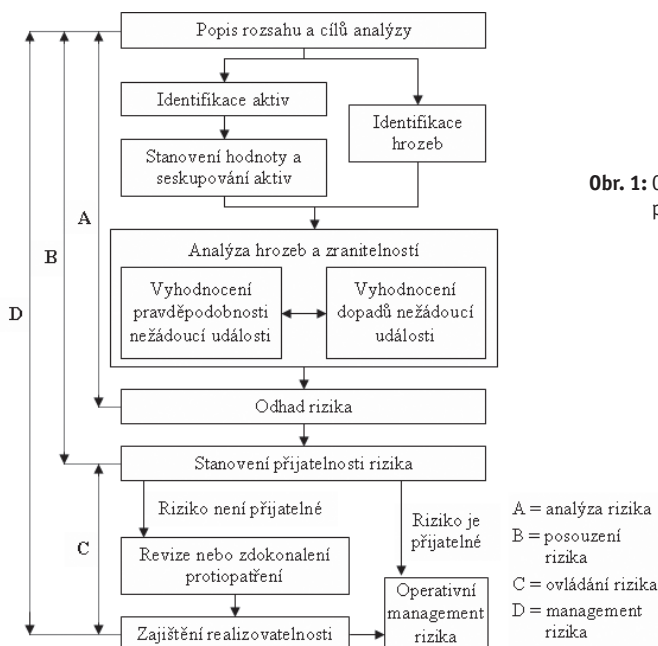
Management rizika je proces, při němž se subjekt snaží analyzovat rizika a s využitím souhrnu získaných informací rozhodnout, která rizika jsou či nejsou přijatelná. Pro identifikovaná

nepřijatelná rizika jsou navrhována protiopatření, která redukuje či eliminují působení již existujících i budoucích faktorů, iniciujících zdroje hrozeb, pomáhají zmírnit dopad nežádoucích událostí a usnadňují rekonstrukci poškozených aktiv či rekonvalescenci ošetřených osob. Obecný postup implementace managementu rizika s vyznačením jeho jednotlivých fází je schematicky znázorněn na obr. 1 [2]. Zmíněný postup lze doporučit k užití nejen na úrovni vojenských útvarů a zařízení, nýbrž i pro potřeby zajištění bezpečnosti jednotlivých sektorů a elementů kritické infrastruktury včetně zabezpečení stability regionů. Konkretizace postupu je dána ponejvíce druhem rizika z aspektu jeho sektorové klasifikace a pro účely využití v AČR by měla být zpracována formou jednotlivých příruček.

2.1 Analýza rizika a její fáze

Primárním předpokladem úspěšného managementu rizik je vymezení cílů a rozsahu analýzy, kde by se mělo vycházet ze záměrů managementu subjektu či potřeb orgánů veřejné a státní správy. V této etapě se začíná také se sběrem informací o posuzovaném subjektu (objektu, systému), jež může pokračovat i v dalších etapách, zejména v průběhu identifikace hrozeb a aktiv, přičemž na základě získaných dat mohou být rozsah i cíle analýzy zpětně modifikovány.

Identifikace hrozeb může probíhat paralelně s identifikací ohrožených aktiv. Spočívá ve zpracování registru (seznamu) hrozeb, které mohou způsobit významnou škodu na životním prostředí, majetku a zdraví vojáků, popř. obyvatel. K tomuto účelu lze užít seznam hrozeb sestavený dle literatury, vlastních zkušeností, výsledků dříve provedených analýz, postupové diagramy, pohovory s vybranými stakeholders [*] a dalšími. Je také možné aplikovat speciální metody v závislosti na skupině sektorových rizik. Pro vojenské útvary lze pro tento účel doporučit aplikaci metody „Check List Analysis“ [3, 4], popř. bezpečnostního auditu [5].



Obr. 1: Obecné fáze řízení rizika a jejich posloupnost

Cílem identifikace aktiv je vytvořit registr zranitelností subjektu (vady a slabiny), jež by mohly být využity potenciálními zdroji hrozeb. Posuzování hodnoty aktiva je založeno na velikosti škody vlivem jeho poškození, zničení či ztráty, vyjadřované v peněžních nebo jiných (ztráta na životech, počet zranění, ztráta biodiverzity ekosystému v procentech aj.) jednotkách. Při oceňování aktiva se berou v úvahu především následující aspekty [2]:

- ❑ pořizovací náklady, resp. reprodukční pořizovací cena,
- ❑ význam aktiva pro existenci či provozování činností subjektu nebo život společnosti,
- ❑ náklady na překlenutí případné škody a rychlost odstranění této škody,
- ❑ výnosové charakteristiky a jiná hlediska, např. potencionální přínosy aktiva.

Kompetentním managerům lze pro identifikaci i stanovení hodnot aktiv doporučit vytvoření, vedení a průběžnou aktualizaci databáze dříve vzniklých škod a skoronehod, které mohou být k těmto účelům pohotově využity. Protože významných aktiv bývá obvykle značné množství, snižuje se jejich počet seskupováním aktiv dle různých hledisek, aby se vytvořily skupiny aktiv podobných vlastností a zjednodušil se celý postup.

Výsledkem analýzy hrozeb a zranitelností by měl být registr dvojic zranitelnost-hrozba s odhadnutou úrovní hrozby a zranitelnosti, jež se v praxi vyjadřují pravděpodobností $P \in (0; 1)$ aktivace zdroje hrozby a vyšší ztráty v důsledku výskytu odtud plynoucí nežádoucí události.

V armádní i civilní praxi je často nezbytné respektovat a zvažovat časovou závislost hodnot pravděpodobnosti výskytu a rozsahu dopadu nežádoucí události. Sumární riziko v časovém intervalu $t \in \langle t_0, t_x \rangle$ lze matematicky charakterizovat vztahem (1).

$$R_{j,i} = \int_{t_0}^{t_x} P_j(t) \times N_{j,i}(t) \times dt \quad (1)$$

nebo alternativně pro časovou závislost rizika rovnicí (2):

$$R_{j,i}(t) = \int_{t_0}^t P_j(\tau) \times N_{j,i}(\tau) \times d\tau \quad (2)$$

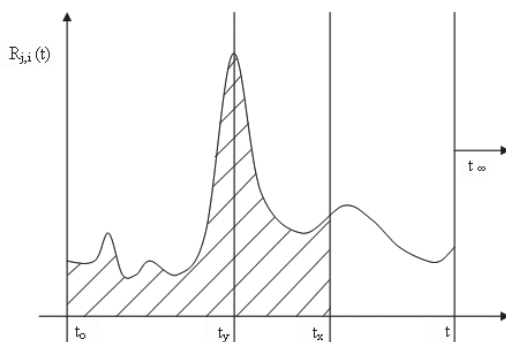
přičemž $P_j(t)$, $P_j(\tau)$ značí funkci pravděpodobnosti výskytu j-té nežádoucí události v závislosti na čase, $N_{j,i}(t)$, $N_{j,i}(\tau)$ časovou závislost výše očekávaných ztrát vlivem průběhu j-té nežádoucí události pro konkrétní aktivum i , $R_{j,i}$ sumární riziko v relaci k j-tému druhu nežádoucí události a i-tému aktivu v časovém intervalu $t \in \langle t_0, t_x \rangle$, $R_{j,i}(t)$ časovou funkci rizika v relaci k j-té nežádoucí události a i-tému aktivu a konečně t , τ jsou symboly pro čas, přičemž ve vztahu (1) $t \in \langle t_0, t_x \rangle$ a ve vztahu (2) $t \in \langle t_0, t_\infty \rangle$.

Graficky je závislost rizika na čase $R_{j,i}(t)$ v souladu s rovnicí (2) demonstrována křivkou na obr. 2 [2]. Šrafovaná plocha pod touto křivkou odpovídá sumárnímu riziku v hodnoceném časovém intervalu $t \in \langle t_0, t_x \rangle$. Z obrázku je současně patrný výrazný nárůst rizika v okolí časové hodnoty t_y , jehož příčinou může být u útvaru např. hromadné doplňování pohonných hmot, střelby apod.

Cílem managementu rizika je minimalizovat sumární riziko, tj. snížit obsah šrafované plochy, vyjadřující sumární riziko $R'_{j,i}$ v časovém intervalu $t \in \langle t_0, t_x \rangle$, resp. vyhledat v tomto intervalu lokální maxima časové funkce. Na redukci rizika v těchto kritických obdobích by měla být ze strany managementu subjektu a priori soustředěna pozornost.

Přejde-li analýza rizika do fáze podrobné kvantitativní studie označované jako *scooping*, budou kladeny vysoké nároky na existenci značného množství přesných vstupních

informací, což proces ekonomicky výrazně zatěžuje. Často však postačí výhradně orientační (kvalitativní) odhad rizika, tzv. *screening*, na základě jehož výsledků je možné učinit rozhodnutí, zda pro identifikovaná kritická rizika bude racionální realizovat další hlubší analýzu (*scooping*).



Obr. 2: Závislost rizika na čase

2.2 Stanovení přijatelnosti rizika

Údaje získané odhadem rizik jsou ve fázi stanovení přijatelnosti rizika porovnávány s referenčními úrovněmi rizik pro jednotlivé druhy nežádoucích událostí. Toto srovnání je podkladem pro přijetí finálního rozhodnutí, zda riziko je či není akceptovatelné a zároveň slouží pro stanovení priorit v relaci k zavádění protipatření pro zvýšení bezpečnosti subjektu (objektu, systému). Při stanovení referenční úrovně rizik je třeba na straně jedné zvažovat pravděpodobnost projevu hrozby a závažnost následků nežádoucích událostí a na straně druhé vycházet z faktu, že absolutní eliminace rizika, tj. dosažení „nulového rizika“ je v praxi zpravidla nereálné, ať již z ekonomických důvodů nebo vzhledem k aktuálnímu stavu vědeckotechnického pokroku.

Výstupem kvalitativního integrovaného posouzení rizik bývá zobrazení rizik v matici rizik, kde jsou rizika vyjádřena buď slovním hodnocením, nebo jak je prezentováno v tab. 1 hodnocením v bodovém systému. Význam bodového hodnocení je uveden v tab. 2 [2]. Uvedený přístup indexového hodnocení rizika lze doporučit k využití i v rozhodovacím procesu velitele vojenské jednotky při přijímání rozhodnutí při plnění bojového úkolu.

Četnost / dopad	1 – zanedbatelný	2 – okrajový	3 – kritický	4 – katastrofický
1 – zanedbatelná	1	2	3	4
2 – malá	2	4	6	8
3 – střední	3	6	9	12
4 – velká	4	8	12	16
5 – velmi velká	5	10	15	20

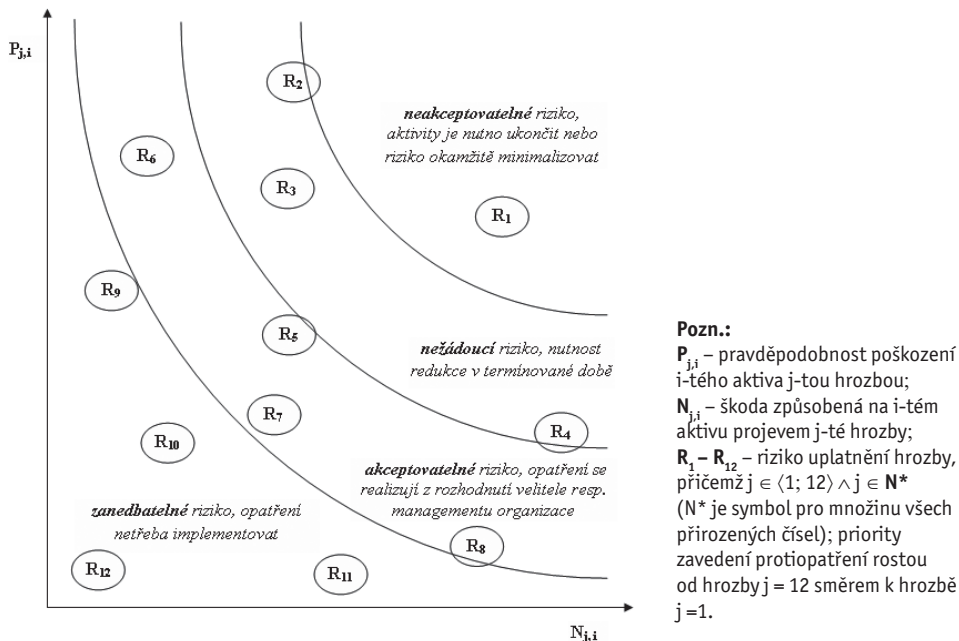
Tab. 1: Matice bodového posouzení rizika nežádoucích událostí

Bodová hodnota	Riziko
1–3	Zanedbatelné. Protipatření není třeba implementovat.
4–7	Akceptovatelné. Protipatření je možnou realizovat se souhlasem vedení posuzovaného subjektu.
8–11	Nežádoucí. Je nezbytné přijmout protipatření v termínované době.
12– 0	Nepřijatelné. Je nutno ukončit aktivitu nebo okamžitě implementovat protipatření na jeho minimalizaci.

Tab. 2: Charakteristika bodové hodnoty rizika

Výstupem integrovaného posouzení rizik může být rovněž grafické vyjádření, často v praxi označované jako mapa rizik. Mapa rizik je demonstrována na obr. 3 [2].

Matice a mapa rizik slouží ke stanovení priorit redukce rizik, vymezení kritických rizik z důvodů zjednodušení a zefektivnění dalších fází managementu rizika a k definování tzv. rizikové pozice vojenské jednotky, ekonomického subjektu nebo regionu.



Obr. 3: Grafické stanovení priorit potřeby minimalizace rizik (mapa rizik)

Pro podporu kvantitativního posuzování rizik se často používají speciální nástroje, zpravidla v podobě programů, mnohdy disponující databází informací, či expertních systémů obsahujících znalostní databáze, kde je algoritmus odhadu rizik již zapracován. Těchto nástrojů existuje pro jednotlivé druhy sektorových rizik řada. Občas bývají uplatňovány i ve standardizovaných vojenských rozhodovacích procesech. Pro správné rozhodnutí v otázce výběru vhodného software je bází precizní znalost aplikovaného algoritmu programu a zároveň aspektu posuzování rizik včetně záměru managementu. V opačném případě může snadno dojít k závažným omylům a nesprávnému vyhodnocení situace.

Pro výběr softwarového produktu, resp. modelu je vždy také nutno zvážit, zda je jeho užití opodstatněné. Rozhodující bývá cíl, který uživatel sleduje, tj. jde-li např. o rychlé zhodnocení situace a stanovení priorit z aspektu okamžitého zásahu anebo o přesnější zjištění s cílem návrhu protiopatření zejména dlouhodobějšího charakteru. Je třeba vždy respektovat zásadu, že získání přesnějších výsledků vyžaduje vyšší množství obvykle specifických a věrohodných dat, jež obvykle nemívá hodnotitel k dispozici a jejichž zajištění bývá časově i finančně náročné. Použití byť přesnějšího modelu, ale při absenci potřebných, dostatečně spolehlivých vstupních dat, může vést analogicky jako při neznalosti algoritmu programu či záměru top-managementu k nesprávným výstupům a následně fatálním chybám v rozhodnutí.

2.3 Ovládání rizika

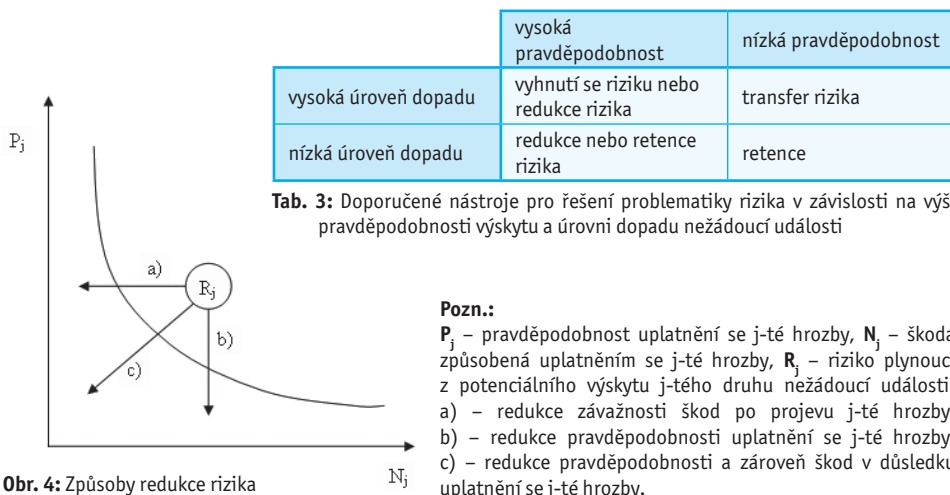
Ovládání rizika je soustavným procesem řízeným top-managementem subjektu, resp. regionu. Je-li riziko neakceptovatelné, zahrnuje proces ovládání rizika revizi nebo zdokonalení protipatření spolu se zajištěním realizovatelnosti navržených protipatření. V opačném případě je realizován proces operativního managementu rizika.

Pro výběr vhodné varianty protipatření a její následnou implementaci, resp. operativního managementu, např. monitoringu rizika, jsou rozhodující účinnost protipatření a jeho ekonomická efektivita vyjadřovaná náklady a přínosy. Ekonomickou efektivitu je nutné vztáhnout na hodnocení finančních, věcných či lidských zdrojů, což se plně promítá i do managementu vojenských systémů. Do nákladů na protipatření, resp. operativní management se započítávají náklady na jeho pořízení, zavedení a provoz, do přínosů pak efekty spojené se zvýšením bezpečnosti. Tento požadavek se v odborné literatuře označuje jako **princip ALARA** (As Low As Reasonably Achievable).

Existují tři základní alternativy redukce rizika. Princip jejich fungování je graficky znázorněn na obr. 4 [2]: a) snížení úrovně dopadu nežádoucí události (nápravná opatření), b) snížení pravděpodobnosti výskytu nežádoucí události (preventivní opatření), c) snížení pravděpodobnosti výskytu a současně dopadu nežádoucí události.

V praxi lze riziko zmírnit pomocí řady nástrojů. Z tohoto pohledu se jeví vysoce účelné zpracovávat a průběžně aktualizovat plány opatření na redukci rizik. Samotný způsob řešení se obvykle odlišuje v závislosti na charakteru rizika, konkrétní situaci, resp. charakteru místních podmínek a finančních, materiálních a personálních možnostech managementu. Obecně lze zmíněné nástroje klasifikovat do čtyř základních kategorií: 1. transfer neboli přesunutí rizika, 2. retence či zadržení rizika, 3. redukce nebo odstranění rizika, 4. vyhnutí se riziku.

Volba nástroje by měla být podřízena vytyčenému cíli a respektovat sumární efektivitu řešení danou nákladovostí implementace protipatření, technickou realizovatelnost, účinnost redukce rizika, sociální a politickou přijatelnost atd. Obecně lze jen stěží doporučit optimální řešení, jež je vždy reflexí konkrétní situace. Nicméně existují jisté zásady v závislosti na výši pravděpodobnosti a úrovni dopadu (tvrdosti) projevu hrozby, jak je patrné z tab. 3 [6].



Obr. 4: Způsoby redukce rizika

Návrh variant možných protiopatření sestává ze dvou základních fází, a sice z návrhu variant protiopatření a následně jejich výběru.

Generace variant se realizuje většinou s využitím některé z invenčních metod, např. brainstorming, brainwriting pool, individuální zápisník nebo Delphi metody.

Pro výběr vhodné varianty z generovaného souboru protiopatření lze doporučit užití multikriteriálního hodnocení. Pro výběr hodnotících kritérií se osvědčuje opět aplikace některé z invenčních metod, pro stanovení vah pak např. aplikace párového hodnocení. Příkladem hodnotících kritérií pro hodnocení variant mohou být následující kritéria:

- ☐ dosažená úroveň bezpečnosti včetně zvážení sekundárních rizik,
- ☐ technická proveditelnost s ohledem na slučitelnost se stávajícím systémem,
- ☐ materiálová efektivnost a energetická náročnost,
- ☐ investiční náročnost,
- ☐ rychlost realizace,
- ☐ pracnost související zejména s nároky na další pracovní síly,
- ☐ úroveň informačního zabezpečení aj.

Pokles rizika vztaženého na vynaložené finanční prostředky bývá zpočátku značný, protože v první etapě lze často implementovat výhradně opatření organizačního charakteru. V pozdější fázi, kdy jsou jednoduchá a finančně nenáročná opatření vyčerpána, se dosahuje poklesu rizika mnohem obtížněji s vynaložením vyšších nákladů.

Při přijímání opatření musí mít rozhodující a finální slovo velitel, popř. vedení správy regionu. Proto je z aspektu efektivního rozhodování nutné, aby top-manageři disponovali adekvátními, jasnými a přehlednými podklady.

Aby byly vyčerpány existující možnosti pro snížení rizika, je nutné vypracovat rigorózní plán realizace konkrétních opatření a prosadit skutečné plnění přijatých plánů. Plány by měly obsahovat následující body:

- ☐ souhrn protiopatření a termíny jejich realizace,
- ☐ rozdělení zodpovědnosti za realizaci každého protiopatření,
- ☐ obsah a termíny školení, resp. výcviku pro jednotlivé stakeholders,
- ☐ program měření pro dokumentaci účinků zavedeného protiopatření.

Důležité je pochopit, že ani pečlivé a obsáhlé posouzení rizik nemůže vést k identifikaci všech rizik a přesnému stanovení pravděpodobnosti a následků dopadu dané nežádoucí události. Proto je nutné provádět operativní management rizika, v rámci jehož realizace se mohou objevit další rizikové události nebo zdroje hrozeb, které dosud nebyly identifikovány. Tento fakt může mít za následek substituční řešení nebo opakování všech fází managementu rizika vzhledem k nově zjištěným skutečnostem.

Jádrem operativního managementu rizika je monitoring a pečlivé vyhodnocování okolí i interního prostředí subjektu, resp. regionu z hlediska rizikových faktorů, které mohou signalizovat vznik rizikových událostí a v případě potřeby iniciovat zavedení korekčních opatření. Monitorovat je třeba hlavně příznaky (spouštěče, aktivátory) rizik, které jsou často nepřímou indikací propuknutí nežádoucí události. V tomto smyslu se jeví účelným identifikovat soubor těchto příznaků, jež obvykle v kratším či delším období před vznikem nežádoucí události zvyšují pravděpodobnost její aktivace. I když někdy nebude reálné nežádoucí událost odvrátit, např. z důvodů krátkodobého příznaku jejího projevu či vzájemné a neočekávané influence hrozeb, bude možné se lépe připravit na zvládnutí nežádoucí situace.

Závěr

Kvalitní naplnění cílů vojenské a bezpečnostní strategie ČR vyžaduje jako jednu z klíčových podmínek implementaci efektivního integrovaného managementu jak v armádní, tak civilní praxi, na úrovni základních subjektů počínaje. Byl předložen postup managementu, který je obecně využitelný nejen ve vojenské, nýbrž i civilní praxi. Je nezbytné zdůraznit, že efektivní management rizik je systematický proces, jenž musí být prováděn průběžně a zvláště při změnách v prostředí, které ovlivňují existenci hrozeb, a tím i celkovou bezpečnost. Má-li být integrovaný management rizik prakticky využitelný a efektivní, je nezbytné především:

- ❑ stanovit odpovědného odborníka nebo tým pro oblast integrovaného managementu rizik, zapojit adekvátním způsobem do procesu všechny stakeholders a zabezpečit regulární vyhodnocování efektivnosti jednotlivých fází subprojektů a finálně celého komplexu managementu rizika,
- ❑ z pozice top-managementu projednávat s tímto týmem aktuální stav v procesu managementu rizik, plánovaná protipatření, připomínky atd.,
- ❑ pravidelně hodnotit adekvátnost posouzení zvláště kritických rizik s akcentem na podrobnost a důslednost, vyhodnocovat efektivnost implementovaných opatření a dosahovanou úroveň bezpečnosti,
- ❑ s výsledky hodnocení seznamovat všechny stakeholders, vždy v rozsahu přiměřeném jejich zastávané pozici a kompetenci,
- ❑ plánovat finanční, materiální a personální zdroje pro zajištění požadované bezpečnosti prostředí, pro školení jednotlivých stakeholders a zavádět vhodné výcvikové programy,
- ❑ zabezpečit efektivní komunikaci rizika,
- ❑ zajistit a vést dokumentaci administrativních podrobností a podstatných zjištění,
- ❑ realizovat pravidelnou kontrolu v oblasti jednotlivých fází managementu rizika.

Poznámka:

- [*] Ad *stakeholders*. Pro daný termín dosud neexistuje adekvátní český ekvivalent. Obecně se jedná o subjekty zainteresované v procesu managementu rizika, tj. rizikové činitele, šířitele rizika, příjemce rizika, subjekty profitující z rizika, subjekty a osoby s formální odpovědností za management rizika, subjekty a osoby s formální odpovědností za reakci na vzniklou nežádoucí událost a zabývající se následky události, informátory o riziku (médiu) aj.

Literatura:

- Vojenská strategie ČR*. Ministerstvo obrany ČR, Praha: Tiskap, 2008. 9 s.
- BOŽEK, F., URBAN, R. *Management rizika: Obecná část*. 1. vyd. Brno: Univerzita obrany, 2008. 145 s. ISBN 978-80-7231-259-7.
- DICKERT, T. G. *Methods for Environmental Impact Assessment*. 1st Edition. Berkeley: University of California, 1974.
- ZAPLETALOVÁ, P., BARTLOVÁ, I., BALOG, K. *Analýza nebezpečí a prevence průmyslových havárií*. 1. vyd. Ostrava: SPBI Spektrum, 1998.
- Bezpečnostní audit*. České ekologické manažerské centrum (CEMC). 1. vyd., Praha: CEMC, 1993.
- SMEJKAL, V., RAIS, K. *Řízení rizik*. 1. vyd. Praha: Grada Publishing, 2003. 270 s. ISBN 80-47-0198-7.